Phòng Chống Tội Phạm Mạng

Tội phạm mạng là một vấn đề nghiêm trọng và ngày càng gia tăng đối với người dùng internet. Mặc dù kết nối trực tuyến rất tuyệt vời, có những điều cần biết để sử dụng internet một cách an toàn. Tội phạm mạng nhắm mục tiêu đến những người mà chúng tin rằng dễ bị tổn thương, bao gồm cả những người bị Khuyết Tật Trí Tuệ và/hoặc Phát Triển. Mọi người nên nhận thức được rủi ro của tội phạm mạng và cách giữ an toàn khi duyệt internet.

Tội Phạm Mạng Là Gì?

Tội phạm mạng là tội phạm thực hiện qua internet trên thiết bị di động (như điện thoại di động), máy tính và mạng Wi-Fi internet công cộng. Tội phạm mạng đánh cắp thông tin nhạy cảm hoặc thông tin cá nhân để thu lợi tài chính.

Các cá nhân được nhắm mục tiêu thông qua nhiều chiến lược khác nhau nhằm thu thập thông tin cá nhân một cách vụng trộm. Nhiều người vô tình mắc phải tội phạm mạng thường bị tổn thất tài chính (trộm cắp), vi phạm dữ liệu cá nhân và đánh cắp danh tính nạn nhân. Biết cách phòng ngừa và tìm kiếm sự trợ giúp sau khi là nạn nhân của tội phạm mạng là điều quan trọng hơn bao giờ hết.

Tội phạm mạng là những kẻ nhân cơ hội và tìm kiếm những nhóm người dễ bị tổn thương để làm con mồi. Với những người bị Khuyết Tật Trí Tuệ và/hoặc Phát Triển (IDD), bọn tội phạm có thể quen biết nạn nhân hoặc tạo sự quý mến như một người quen hoặc người đáng tin cậy.

Các Loại Tội Phạm Mạng Phổ Biến

Tấn Công Giả Mạo: Sử dụng email, tin nhắn văn bản và cuộc gọi điện thoại để khiến nạn nhân tiết lộ thông tin cá nhân hoặc tài chính và/hoặc thông tin đăng nhập.

Không Giao Hàng: Sử dụng internet để gạ gẫm thanh toán điện tử bất hợp pháp cho việc mua hàng hóa và dịch vụ, sau đó nạn nhân sẽ không bao giờ nhận được hàng.

Tống Tiền: Lấy tiền hoặc hàng hóa bằng cách hăm dọa hoặc mối đe dọa từ một người nào đó giả mạo là người của một cơ quan có thẩm quyền (như IRS). Các mối đe dọa có thể bao gồm gây tổn hại thân thể, truy tố hình sự hoặc phơi bày ra công chúng. Nó cũng có thể liên quan đến việc khóa quyền truy cập vào dữ liệu của nạn nhân và giữ nó để đòi tiền chuộc.

Vi Phạm Dữ Liệu Cá Nhân: Đánh cắp và chia sẻ dữ liệu và thông tin cá nhân riêng tư của một cá nhân cho người dùng trái phép.

Trộm Cắp Danh Tính: Đánh cắp và sử dụng thông tin cá nhân của một cá nhân khác để thực hiện hành vi gian lận hoặc các tội phạm khác.

Bản Tin Sức Khỏe Và An Toàn do Sở Dịch Vụ Phát Triển ấn hành để cảnh báo cho các nhà cung cấp dịch vụ trực tiếp, các trung tâm khu vực và những người khác về những rủi ro cụ thể được xác định trong cộng đồng của chúng ta.

Vui lòng cung cấp phản hồi về bản tin này và những gì chúng tôi có thể làm tốt hơn thông qua khảo sát này: Khảo Sát Về Bản Tin

Tội Phạm Mạng Ở Hoa Kỳ Vào Năm 2020

- Trong đại dịch COVID, những người bị IDD là nạn nhân của bọn tội phạm mạng, những kẻ này đã chuyển hướng tiền viện trợ kích thích kinh tế của liên bang được gửi đến cho họ bằng phương thức điện tử.
- California có số lượng đơn khiếu nại tội phạm mạng cao nhất trên toàn quốc.
- FBI đã nhận được gần 800.000 đơn khiếu nại về tội phạm mạng từ công chúng, **tăng 69%** so với năm trước.
- Tấn công giả mạo là cuộc tấn công mạng phổ biến nhất với hơn **241.000** nạn nhân được báo cáo.
- Các khoản mất mát được báo cáo đã vượt quá **$4,1 tỷ**.
- Những người trên 60 tuổi là nạn nhân nhiều nhất so với bất kỳ nhóm tuổi nào.

Giúp Bảo Vệ Các Cá Nhân Mà Bạn Phục Vụ Khỏi Tội Phạm Mạng

Internet là một không gian công cộng

Nhắc nhở người tiêu dùng phải hết sức cẩn thận trước khi chia sẻ thông tin cá nhân, như số an sinh xã hội, thông tin tài khoản ngân hàng và thông tin y tế trên internet.

- **Phải luôn sử dụng mạng Wi-Fi công cộng một cách thận trọng.**
- Mạng Wi-Fi công cộng được mở cho bất kỳ ai nếu họ nằm trong phạm vi phủ sóng và thường không yêu cầu người dùng đồng ý với bất kỳ điều khoản hoặc điều kiện nào trước khi kết nối.

- Mặc dù sử dụng Wi-Fi công cộng rất tiện lợi nhưng nó thường có bảo mật kém. Điều này có nghĩa là thông tin cá nhân (như tên người dùng và mật khẩu), có thể bị người khác xem được bằng phương pháp điện tử mà nạn nhân không hề hay biết.
- Mạng Wi-Fi bảo mật thường yêu cầu mật khẩu người dùng và có thể phải trả phí hoặc mua để sử dụng.

Sử Dụng Mật Khẩu Mạnh Cho Tài Khoản Trực Tuyến

Giúp những người mà bạn phục vụ tạo mật khẩu mạnh.

- Khuyến khích người tiêu dùng không sử dụng mật khẩu phổ biến hoặc mật khẩu có thể dễ dàng đoán được.
- Mật khẩu mạnh có ít nhất 8 ký tự và bao gồm sự kết hợp của chữ hoa và chữ thường, ký hiệu và số. Mật khẩu càng dài thì càng an toàn.
  - **Mật khẩu yếu**: “password”, tên hoặc ngày sinh của bạn, 12345,
  - **Mật khẩu mạnh**: 8blu3Car$dr1vinG, 1&n%00Xb#, Y3!!oWfL0w3rs

Kiểm tra cài đặt quyền riêng tư thường xuyên

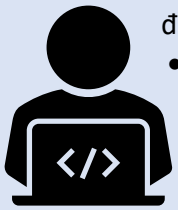
Giúp những người mà bạn phục vụ kiểm tra cài đặt quyền riêng tư trên thiết bị di động và máy tính của họ. Giải thích cách thiết lập Xác Thực Hai Yếu Tố bằng cách điều chỉnh cài đặt quyền riêng tư trên tài khoản trực tuyến. Xác Thực Hai Yếu Tố là người dùng được gửi một văn bản hoặc email có mã đặc biệt mỗi khi cá nhân đăng nhập vào tài khoản trực tuyến của họ.

Bản Tin Sức Khỏe Và An Toàn do Sở Dịch Vụ Phát Triển ấn hành để cảnh báo cho các nhà cung cấp dịch vụ trực tiếp, các trung tâm khu vực và những người khác về những rủi ro cụ thể được xác định trong cộng đồng của chúng ta.

Vui lòng cung cấp phản hồi về bản tin này và những gì chúng tôi có thể làm tốt hơn thông qua khảo sát này: Khảo Sát Về Bản Tin

Vi-rút Và Phần Mềm Độc Hại

- ***Phần mềm độc hại*** là một loại phần mềm được thiết kế để gây hại cho thiết bị di động hoặc hệ thống máy tính.



  - ***Vi-rút*** là mã máy tính xâm nhập vào hệ thống máy tính mà không được cho phép và "lây nhiễm" cho máy tính. Chúng ẩn trong các tệp hoặc ứng dụng được gửi qua email hoặc tin nhắn văn bản và lây nhiễm vào máy tính khi chúng được mở. Vi-rút là một loại phần mềm độc hại.
- Vi-rút có thể lấy cắp thông tin người dùng, làm chậm và làm hỏng máy tính hoặc kiểm soát hoàn toàn máy tính hoặc thiết bị.
- Vi-rút không thể tự lây lan. Chúng lây lan khi mọi người vô tình chia sẻ chúng. Điều này thường xảy ra khi chia sẻ các tệp hoặc email bị nhiễm.

Phải Làm Gì Sau Khi Trở Thành Nạn Nhân Của Tội Phạm Mạng

Giải thích tầm quan trọng của việc gọi đến ngân hàng của họ và hủy thẻ ghi nợ hoặc thẻ tín dụng bị nhắm đến trong cuộc tấn công mạng. Giúp thay đổi thông tin đăng nhập cho các tài khoản trực tuyến. Cảnh báo cho tổ chức quản lý tài khoản bị tấn công về cuộc tấn công và hỏi về bất kỳ khoản phí gian lận nào được ghi có.

Bộ Công Cụ Sức Khỏe DDS có thêm thông tin về cách hỗ trợ và bảo vệ các cá nhân mà bạn phục vụ.

Nguồn Lực Hữu Ích

Thi Hành Luật Địa Phương

Trung Tâm Khiếu Nại Tội Phạm Internet (IC3)

Ủy Ban Thương Mại Liên Bang (FTC)

- Báo cáo gian lận tại ReportFraud.ftc.gov
- Gọi cho đường dây nóng của FTC theo số 1-877-IDTHEFT (1-877-438-4338)
- Báo cáo hành vi trộm cắp danh tính và tìm thêm thông tin tại identitytheft.gov

Suy Nghĩ Trước Khi Nhấp Vào

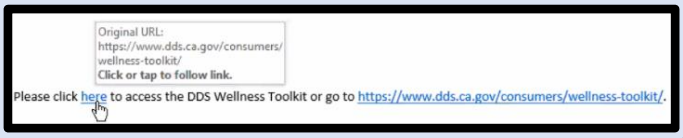
- Can ngăn những người mà bạn phục vụ mở các tệp đính kèm không được yêu cầu hoặc nhấp vào các liên kết không thể nhận dạng. Các tệp đính kèm hoặc liên kết này có thể dẫn đến vi-rút hoặc phần mềm độc hại sẽ gây hại cho máy tính.
- Cảnh báo người tiêu dùng nên thận trọng trước khi nhấp vào các liên kết trông giống như trò chơi hoặc lời hứa hẹn nhận được quà "miễn phí" nếu họ nhấp vào liên kết.
- Khuyến khích người tiêu dùng kiểm tra địa chỉ email họ nhận được để xác nhận rằng người gửi là hợp pháp. Nếu họ nhận được một email bất ngờ với các liên kết hoặc tệp đính kèm, hãy đề nghị họ liên hệ với người gửi qua điện thoại hoặc tin nhắn để xác nhận rằng chính người gửi đã gửi email.
- Tấn công giả mạo là một hình thức lừa đảo phổ biến trên internet nhằm lừa những người chia sẻ thông tin cá nhân của họ thông qua việc sử dụng các tin nhắn giả trông giống như thật.

  - Trước khi trả lời bất kỳ thư nào, hãy lưu ý các dấu hiệu nhận biết của một trò lừa đảo tấn công giả mạo: người gửi không quen thuộc, lỗi chính tả và ngữ pháp, các liên kết đáng ngờ không khớp với nội dung của thư, các tệp đính kèm ngẫu nhiên, nội dung email với cảm giác cấp bách.

Trước Khi Trả Lời Hoặc Nhấp Vào Email

Khuyến khích người tiêu dùng xác minh ai đang gửi email cho họ.

- Kiểm tra địa chỉ email của người gửi bằng cách di chuyển con trỏ qua tên của họ hoặc liên kết để đảm bảo rằng địa chỉ này có vẻ như đến đúng doanh nghiệp.



Bản Tin Sức Khỏe Và An Toàn do Sở Dịch Vụ Phát Triển ấn hành để cảnh báo cho các nhà cung cấp dịch vụ trực tiếp, các trung tâm khu vực và những người khác về những rủi ro cụ thể được xác định trong cộng đồng của chúng ta.

Vui lòng cung cấp phản hồi về bản tin này và những gì chúng tôi có thể làm tốt hơn thông qua khảo sát này: Khảo Sát Về Bản Tin